(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
30 August 2001 (30.08.2001)

PCT

(10) International Publication Number
WO 01/63994 A2

(51) International Patent Classification[7]: H05K 5/00

(21) International Application Number: PCT/US01/05912

(22) International Filing Date: 22 February 2001 (22.02.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/510,825 23 February 2000 (23.02.2000) US

(71) Applicant: IRIDIAN TECHNOLOGIES, INC. [US/US]; Suite E, 9 East Stow Road, Marlton, NJ 08053-3159 (US).

(72) Inventors: VAN SANT, Glen; 414 Valley Road, Langhorne, PA 19047 (US). MASSARI, Angelo; 696 Oak Avenue, Malaga, NJ 08328 (US).

(74) Agents: DONOHUE, John, P., Jr. et al.; Woodcock Washburn Kurtz Mackiewicz & Norris LLP, 46th Floor, One Liberty Place, Philadelphia, PA 19103 (US).

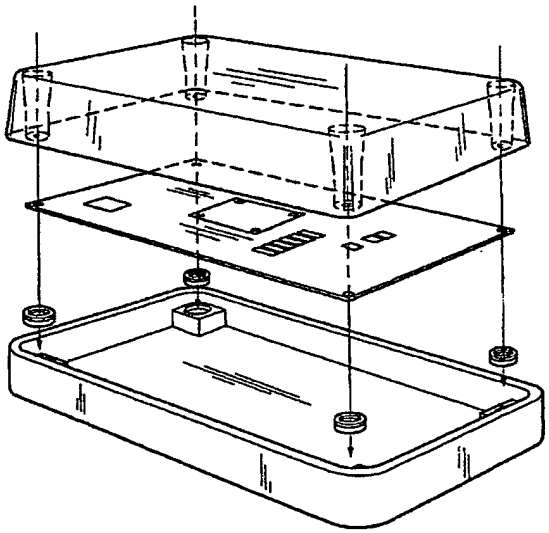
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: TAMPER PROOF CASE FOR ELECTRONIC DEVICES HAVING MEMORIES WITH SENSITIVE INFORMATION



(57) Abstract: A tamper-proof enclosure is disclosed. The enclosure utilizes various types of sensors that are capable of detecting chassis intrusion, extreme temperature variations and low battery power. A circuit is formed when the chassis is closed and broken when the chassis is opened. A sensor connected to the circuit detects a broken circuit. Other sensors detect unacceptable high or low temperatures and low battery power. When a sensor detects such a condition, it sends a signal causing a portion of the memory of the device contained within the enclosure to be erased.

WO 01/63994 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE

TAMPER PROOF CASE FOR ELECTRONIC DEVICES HAVING MEMORIES WITH SENSITIVE INFORMATION

Field of the Invention

The invention relates to a tamper proof case for devices that have a memory containing sensitive information.

Background of the Invention

There are many computer controlled devices which have memories containing sensitive information. Such information could range from financial information to encryption keys, to passwords. Such devices may be in areas that are accessible to the public or which could be entered by anyone who wants the information. Consequently, there have been concerns about unauthorized access to the devices and retrieval of the sensitive information by a thief. Thus, there is a need for a tramper proof case which will prevent unauthorized access to sensitive information.

Several types of tamper proof enclosures have been developed. One type of enclosure contains a seal which is broken when the enclosure is opened. The seal will indicate whether a container has been opened but it does not prevent removal of sensitive

information from the enclosure after opening. Another type of enclosure contains an alarm which sounds when the case or door is opened. While the alarms may promptly alert authorities of a breach, the sensitive information is still available to the thief when the enclosure is opened, provided he can quickly retrieve it and escape.

Erasable memories are well known. Where sensitive information is contained in a memory, one way to deter theft of information is to erase the memory whenever the thief or other unauthorized person seeks access. However, prior to the present invention, the art had not developed a tamper-proof case which would cause a memory to be erased when the case was opened.

Summary of the Invention

A system which determines the identity of individuals utilizing an iris scan device contains a cryptographic sub-system that encrypts digitized iris scans prior to transporting them to a remote facility for verification or matching with known samples. Information in encrypted form may also be received by the system. Such a system could be used, for example, to positively identify individuals wishing to access an automated teller machine or to gain access to a restricted facility. Both encryption and decryption require the use and storage of encryption/decryption keys for extended periods of time. Because we do not want the encryption/decryption keys to be compromised, there is a requirement for physical key security.

A tamper-proof case is disclosed herein. If tampering is detected, the sensitive information, such as encryption/decryption keys, is deleted or zeroed out. Three forms of tampering are sensed: chassis intrusion, extreme temperature conditions and low battery power. The case may utilize one or more of several methods, described below, to detect tampering. The case itself consists of a metal enclosure having two or more parts which are joined together to form the whole enclosure. The components of the device, including the circuitry which contains the sensitive information, reside within the enclosure.

The first method of detecting tampering consists of a conductive ring which must make simultaneous contact with a plurality of conductive portions, or traces, on the printed circuit board. When two halves of the enclosure are separated, the conductive ring

no longer makes contact with all of the conductive portions of the printed circuit board, and the tampering is detected.

The second method of detecting tampering is designed to protect all or part of a printed circuit board, specifically, a board or portion of a board containing memory chips storing sensitive information. This method utilizes a protective conductive mesh which encloses the circuit board. If the mesh is pierced, an open circuit condition is generated, and the tampering is detected. This prevents physical intrusion through the walls of the enclosure, such as by drilling or sawing.

A third method of preventing tampering involves the use of a temperature detector to detect extremes in temperature. This will defeat any attempts to "freeze" components of the device within the enclosure by lowering the temperature to a level where the devices will not work, thereby allowing time to access the components before the memory can be erased. If the temperature detector detects a temperature outside of a specific range of acceptable temperatures, the memory of the device is immediately erased.

Lastly, a device is utilized which detects a low battery condition. Ideally, in a loss of power situation, the device's internal batteries will provide power to the circuitry that protects the memory containing the sensitive information. Should these batteries run low, it would be possible to gain access to the sensitive information merely by removing power from the device. When a low battery condition is detected, the sensitive information in the memory device is erased.

Description of the Drawings

Figures 1a, 1b and 1c show various views of the conductive annulus used in the security switch.

Figure 2 is an exploded view of the tamper proof case with showing the placement of the security switches.

Figure 3 is a cutaway view of a corner of the bottom portion of the tamper-proof case showing a portion of the security switch.

Figure 4 shows the portion of the security switch in place on a printed circuit board.

Figures 5a and 5b show a frame used to protect specific areas of a printed circuit board.

Figures 6a and 6b show a second embodiment of the frame of Figures 5a and 5b.

Figure 7 shows the frame of Figures 6a and 6b in dotted outline in place on a printed circuit board.

Detailed Description of the Invention

The body of the case, in the preferred embodiment, consists of two halves, 14 and 16, best shown in Figure 2. These are preferably composed of a metal such as cast aluminum, but any hard material may be used, such as hard plastic. The two halves 14 and 16 of the case are fitted together to form the whole case. Inside the case is a main circuit board 18 which contains the circuitry of the device plus additional security monitoring circuitry. Several switches are implemented as part of the electrical traces of circuit board 18. In the preferred embodiment, these switches consist of an electrical trace shaped like an annulus divided into two or more segments. These are best shown in Figure 4 as reference numbers 22. Annular segmented contact 22 is printed around hole 23 in circuit board 18. All segments of annular contact 22 must make contact with a conductive ring 10 (external to the circuit board), shown in Figure 1, for the switch to be closed. Hole 23 in annular contact 22 is used for mounting the circuit board to the interior of the case as well as for providing the mounting constraints for conductive ring 10 used to close the switches.

One half 16 of the case contains one or more bosses 20 that permit one or more mounting screws to pass through the circuit board and thread into the other half of the casing 14, which has corresponding bosses 17 defined therein. Located at the top of one boss of each pair of bosses 20 and 17 is an annulus of resilient material 12, preferably composed of foam or sponge rubber, and which, in the preferred embodiment, is approximately .08 inches thick. Rubber annulus 12 has a contact adhesive applied to both sides. Each rubber annulus 12 is attached to the top of a boss 20 on one half 16 of the casing. The ring shape permits mounting screws to pass through the circuit board 18 and into boss 20. As shown in Figure 1, conductive washer 10 is attached to the other side of rubber annulus 12, thereby forming washer/annulus assembly 8. Circuit board 18 is then

mounted on top of conductive washers 10, with the washers contacting circuit board 18 at the places where annular contacts 22 are printed.

All of the switches on the circuit board are connected in series by conductive traces 15. The switches are part of a monitoring circuit, which is electrically closed when all of conducting washers 10 join all segments of each annular contact 22. The segments of each annular contact 22 are joined when conductive washers 10 are compressed against the circuit board 18 by rubber annuli 12, mounted on bosses 20 on one half 16 of case when the two halves of the case 14 and 16 are secured to each other by the mounting screws (not shown). The normal operation of the system is such that each switch is closed, thus completing the circuit. If any switch is opened, by the removal of conductive washer 10 from annular contact 22, the circuit will open and the resulting absence of current will be detected by a sensor. A switch is opened when any attempt is made to separate the two halves 14 and 16 of the case. Such attempts will cause conductive washers 10 to pull away from the annular contacts 22 on circuit board 18, thereby opening the monitoring circuit.

The monitoring circuit is designed to detect an opening of one or more of the switches, which indicates an attempt to tamper with the contents of the case. When such a condition is detected, any important or sensitive data contained within the circuitry of circuit board 18, such as encryption keys on a cryptography module, are erased. The monitor circuit is powered by a battery located on circuit board 18. The presence of the battery ensures that protection of the sensitive data also exists if the system is powered down.

A key component of this switch arrangement is the mounting of conductive washers 10 for the switches. Each conductive washer 10 is bound to a rubber annulus 12 mounted on the cover bosses 20 via a contact adhesive, forming assembly 8. The thickness of each assembly 8 is greater than the clearance between the annular contacts 22 of on circuit board 18 and boss 20. This causes rubber annulus 12, which is resilient, to compress as the two halves 14 and 16 the case are secured together via mounting screws. The mounting screws which will extend through boss 17, defined in half of cover 14, circuit board 18 and annular contact 22, conductive washer 10, rubber annulus 12 and boss 20. The screws may be secured by nuts applied on the underside of boss 20, or may screw

directly into threads defined in boss 20. As it compresses, rubber annulus 12 pushes conducting washer 10 onto annular contact 22 on circuit board 18, thereby keeping conductive washer 10 forced into contact with each segment of annular contact 22, completing the circuit. If either cover 14 or 16 is lifted or tilted in an effort to look into or access the interior of the case, conductive washer 10 will lift from annular contact 22 and break the circuit, resulting in the deletion of the sensitive data. The more segments in annular contact 22, the more sensitive the switch is to tampering. For instance, by having eight segments, it is relatively difficult to tilt either half 14 or 16 of the case in any direction and keep conductive washer 10 touching all segments of annular contact 22.

This same technology can also be used to protect specific areas of the circuit board. For example, in Figures 5a and 5b, an aluminum frame is shown which fits around the portion of circuit board 18 housing the circuitry containing the sensitive data. In this case, two or more pairs of contacts 34, shown in Figure 7, are laid out on circuit board 18 surrounding the area which is to be protected. Resilient foam rubber gasket 26 of the same shape as frame 24 holds frame 24 in place on circuit board 18, thereby connecting all of segments 34, when the halves 14 and 16 of the case are joined together. A boss on half 14 of the case, shaped similarly to frame 24 will compress resilient foam rubber gasket 26 and force frame 24 into contact with contacts 34. Any attempt to separate the halves 14 and 16 of the case causes frame 24 to pull away from circuit board 18, breaking the contact with contacts 34 and opening the circuit. In an alternative embodiment, metal frame 24 could be replaced with a conductive foil tape 32, shown in Figure 6b, which is attached to a foam rubber frame 30 via a contact adhesive in the areas where foam rubber frame 30 touches contacts 34 on circuit board 18. Figure 7 shows foam rubber frame 30 in dotted outline in place on circuit board 18, with conductive foil patches 32 joining contacts 34 on circuit board 18.

Another method used to protect the portion of the circuit board containing the cryptography circuit is covering the circuitry with a conductive sheet or mesh (not shown). The sheet utilizes conductive traces (ink or metal for example) forming a grid pattern. The grid is connected in parallel to the edges of the sheet and connected to an electrical supply forming another monitor circuit. If one or more of the traces in the grid are broken by any form of penetration, such as drilling or sawing, the circuit will be

broken, resulting in the deletion of the sensitive data. An example of a conducting mesh suitable for use in this application is manufactured and sold by W. L. Gore & Associates, Ltd., under the trade name D^3 Technology. The mesh would cover both sides of the circuit board to prevent access to the board by drilling or cutting of the case around the board.

During normal operations, normal operating power is supplied to circuit board 18. Should normal power be interrupted for any reason, be it an attempt to disable the unit by turning off its power supply, or a normal power outage, the circuitry in which the sensitive data is stored and the security monitor circuitry on circuit board 18 remains powered by an on-board battery. A sensor is located on circuit board 18 which detects when the on-board battery runs low on power.

Although any method may be used to delete the sensitive data from the memory of the particular device which has been placed into the tamper-proof case, the iris scan device described above utilizes a microcontroller which operates in zero-power "sleep" mode. The sensitive data in this case is one or more cryptography key, which are stored in SRAM. Both the microcontroller and the SRAM can be powered utilizing battery power when normal power is unavailable. The occurrence of any security violation generates an interrupt to the microcontroller which, following a transition from zero-power (sleep mode) to low-power mode, destroys all keys via an erasure/overwrite by software of the SRAM chip. The time to transition from zero power to low power mode is approximately on the order of microseconds, and the time to perform SRAM erasure/overwrite by software is a few milliseconds. Hence, the keys are erased well before anyone could successfully intrude into the security module.

The low battery power detection feature ensures that the microcontroller has sufficient power to perform the destruction of the sensitive data upon detection of an intrusion. Should the battery power drop below this threshold, the microcontroller will erase all sensitive data as a safeguard.

The final safeguard is a temperature sensor that resides within the case. The temperature sensor is primarily designed to guard against the type of attack wherein someone would try to freeze the electronics of the device with liquid nitrogen to shut down the security monitoring circuitry, thereby allowing the attacker to access the cryptography circuitry before the security monitoring circuitry could delete the sensitive data. The same

would apply to a high temperature attack. Therefore, the temperature sensor is tuned to alert the microcontroller to delete the keys if the temperature is outside of a given range, which, in the preferred embodiment, is approximately 0c - 65c. In a normal operating environment, such as the inside of an ATM machine, a certain ambient temperature must be maintained. The temperature range of the temperature sensor covers the expected range of operating temperatures in various normal operating situations.

In the preferred embodiment of the device, all of the described anti-attack measures will be present, however, the invention is not limited thereto, and may include embodiments that have a subset of the measures described. Furthermore, it should be distinctly understood that our invention is not limited thereto but may be variously embodied within the scope of the following claims.

I claim:

1. A tamper-proof case for a device having a memory containing information comprised of:

an enclosure having at least two mating parts which fit together to define an enclosed space, wherein said device having a memory containing information is disposed within said space;

at least two electrical contacts, positioned such that said contacts are electrically coupled, thereby forming a current path, when said first and said second mating parts are joined together and electrically uncoupled, thereby interrupting said current path, when said first and said second mating parts are separated; and

a sensor for sensing a flow of electrical current through said current path, said sensor being capable of sending a signal when said electrical contacts are uncoupled, said signal causing said device to erase at least a portion of said information from said memory.

2. The tamper-proof case of claim 1 wherein said at least two electrical contacts are traces on a printed circuit board.

3. The tamper proof case of claim 2 further comprising:

a piece of electrically conductive material; and

a piece of resilient material, secured to said piece of electrically conductive material and to one of said mating parts, and disposed therebetween;

such that said piece of electrically conductive material is biased by said piece of resilient material against said at least two electrical contacts, thereby electrically coupling said

contacts, when said at least two mating parts are joined together.

4. The tamper-proof case of claim 3 wherein said piece of resilient material is foam rubber.

5. The tamper-proof case of claim 4 wherein:

said printed circuit board defines a hole therein; said at least two electrical contacts are laid out as a circle on a printed circuit board around said hole; and

said piece of electrically conductive material is a metal annulus sized to match said circle defined by said at least two electrical contacts.

6. The tamper proof case of claim 5 further comprising:

a first boss, defined in one of said at least two mating parts, said boss defining a hole therein;

wherein said foam rubber is annular in shape and disposed between said metal washer and said first boss.

7. The tamper proof case of claim 6 further comprising:

a second boss, defined in the other of said at least two mating parts, said second boss defining a hole therein, wherein said first and said second bosses are aligned when said at least two mating parts are joined together; and

a screw, disposed through said hole in said first boss, said hole in said printed circuit board, said hole in said metal annulus, said hole in said foam rubber annulus and said hole defined in said second boss, such that when said screw is tightened, said at least two mating parts are joined together and said foam rubber annulus is compressed, thereby biasing said metal annulus against said at least two electrical contacts defined as traces on said printed circuit

board, and electrically coupling said electrical contacts and forming a switch which is electrically closed when said at least two mating parts are joined and electrically opened when said at least two mating parts are separated.

8. The tamper proof case of claim 7 further comprising a plurality of said switches.

9. The tamper-proof case of claim 4 wherein:

said piece of electrically conductive material is a piece of metal tape bonded to said piece of foam rubber; and

said piece of foam rubber is bonded to one of said at least two mating parts, such that when said at least two mating parts are joined together, said foam rubber biases said metal tape against said electrical contacts, thereby electrically coupling said electrical contacts.

10. The tamper-proof case of claim 1 further comprising:

an electrically conductive mesh disposed within said case such that at least said portion of said device containing said memory is covered by said mesh; and

a sensor for detecting if said mesh has been pierced, said sensor being capable of sending a signal when said mesh has been pierced, said signal causing said device to erase at least a portion of said information from said memory.

11. The tamper-proof case of claim 1 further comprising:

a temperature sensor for determining the ambient temperature within said case, wherein said temperature sensor generates a signal if said ambient temperature exceeds a predetermined maximum temperature or if said ambient temperature drops below a predetermined minimum temperature, said signal causing said

device to erase at least a portion of said information from said memory.

12. The tamper-proof case of claim 11 wherein said maximum temperature is 65 degrees centigrade and wherein said minimum temperature is 0 degrees centigrade.

13. The tamper-proof case of claim 1 further comprising:

an internal battery capable of delivering a voltage; and

a sensor for detecting when said voltage drops below a certain predetermined minimum voltage, said sensor being capable of sending a signal when said voltage drops below said predetermined minimum, said signal causing said device to erase at least a portion of said information from said memory.

14. A tamper-proof case for a device having a memory containing information comprised of:

an enclosure having at least two mating parts which fit together to define an enclosed space, wherein said device having a memory containing information is disposed within said space;

a first electrical contact on a first mating part of the at least two mating parts, a second electrical contact on a second mating part, the second electrical contact positioned to engage the first electrical contact when the first mating part and the second mating part are joined together;

a power source connected to said first electrical contact such that an electrical circuit is formed when the first and second mating parts are joined together;

a sensor in the electrical circuit which senses flow of electrical current through the circuit and sends a signal when such electrical current is interrupted which signal causes the device to erase at least some information from the memory.

15. The tamper-proof case of claim 1 also comprising:

a mesh adjacent at least one of the enclosure, the mesh having conductive traces connected to the power source to form a circuit so that electricity flows through the conductive traces;

a sensor connected to the conductive trances which senses flow of electrical current through the circuit and sends a signal when such electrical current is interrupted which signal causes the device to erase at least some information from the memory.

16. The tamper-proof case of claim 15 wherein the mesh is adjacent all inside surfaces of the enclosure.

17. The tamper-proof case of claim 14 also comprising a circuit board attached to the first mating part, the circuit board containing the first electrical contact and a conductive trace connected to the first electrical contact, the power supply and the sensors, the conductive trace having a gap sized and positioned to mate with the second electrical contact and thereby complete an electrical circuit.

18. The tamper proof case of claim 14 comprising a resilient washer connected to the second mating port and carrying the second electrical circuit.

19. The tamper proof case of claim 18 wherein the second electrical contact is annular.

20. The tamper proof case of claim 19 wherein the second electrical contact is segmented and the first electrical contact is segmented such that the segments of the first electrical contact are sized and positioned to meet and engage the segments of the second electrical contact to complete the electrical current when the first and second mating parts are joined.

21. The tamper proof case of claim 20 wherein the second electrical contact has eight segments.

22. The tamper proof case of claim 14 also comprising a temperature sensor within the enclosure, the temperature sensor designed to emit a signal when temperature within the enclosure falls below a preselected minimum temperature.

23. The tamper proof case of claim 14 also comprising a battery and a battery power detector connected to the battery, the battery and battery power detector connected to the battery, the battery and battery power detector being within the enclosure and wherein the battery power detector sends a signal when the battery reaches a power level below a predetermined power level, this signal causing the device to erase at least some information from the memory.

24. The tamperproof case of claim 14 wherein the memory contains encryption keys which are erased when a signal is sent by the sensor.

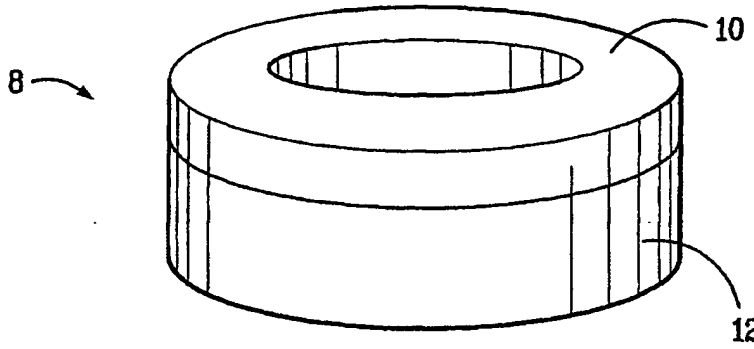


FIG. 1A

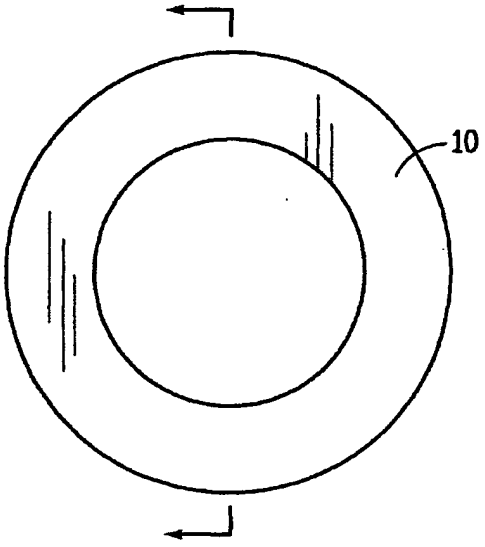


FIG. 1B

FIG. 1C

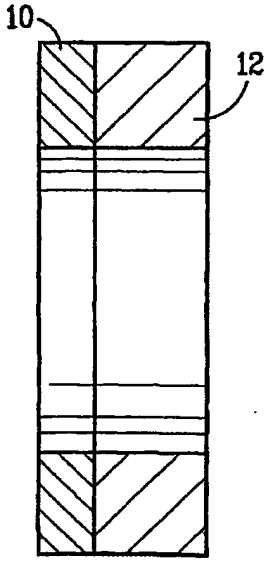
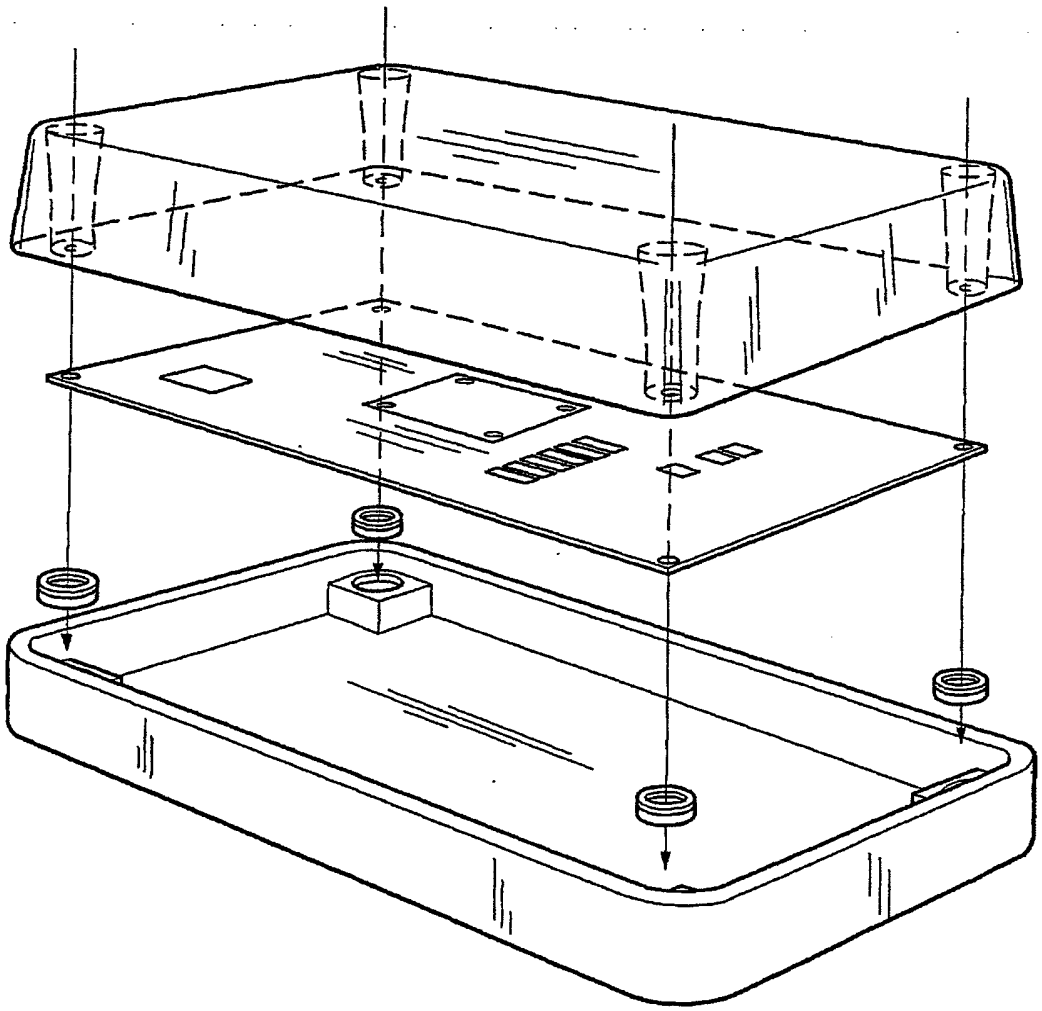


FIG. 2



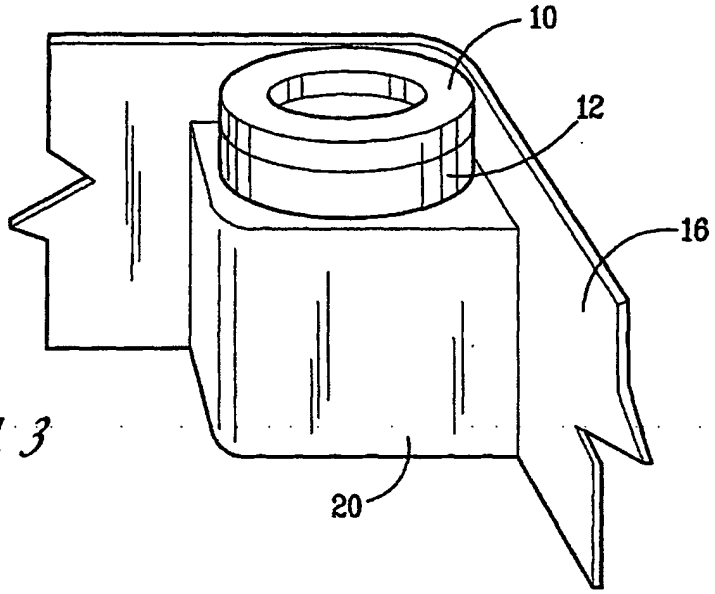


FIG. 3

FIG. 4

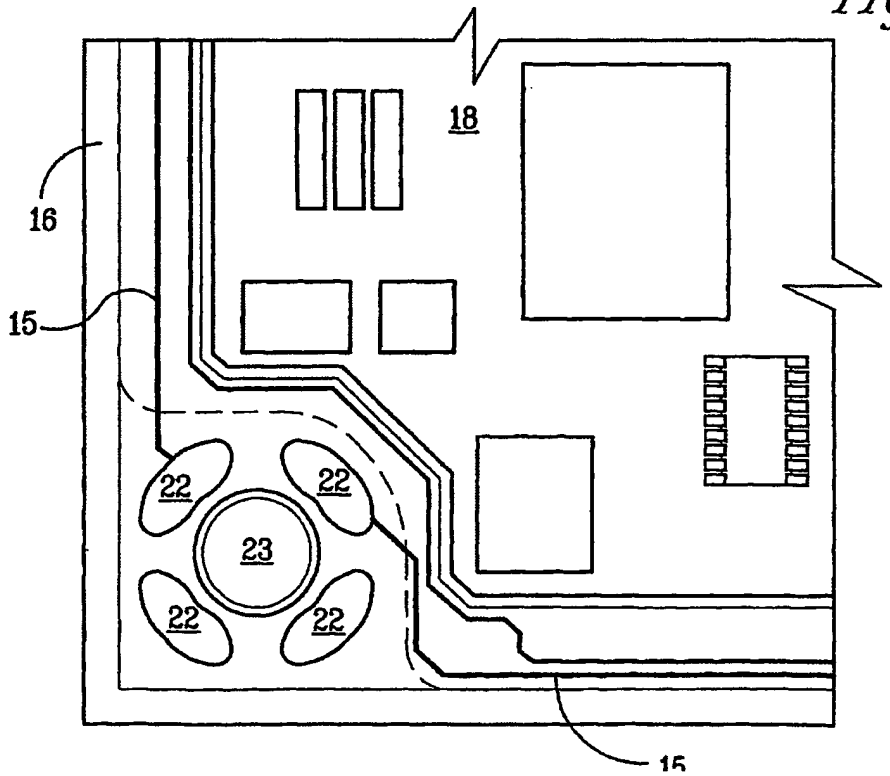
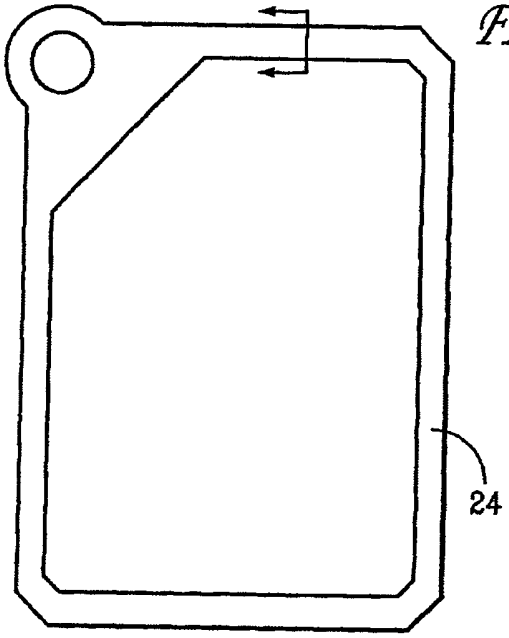


FIG. 5A



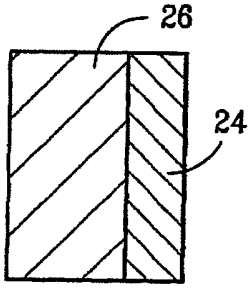


FIG. 5B

FIG. 6A

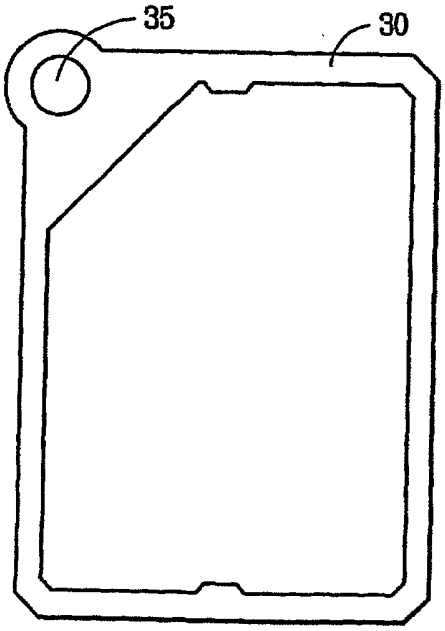


FIG. 6B

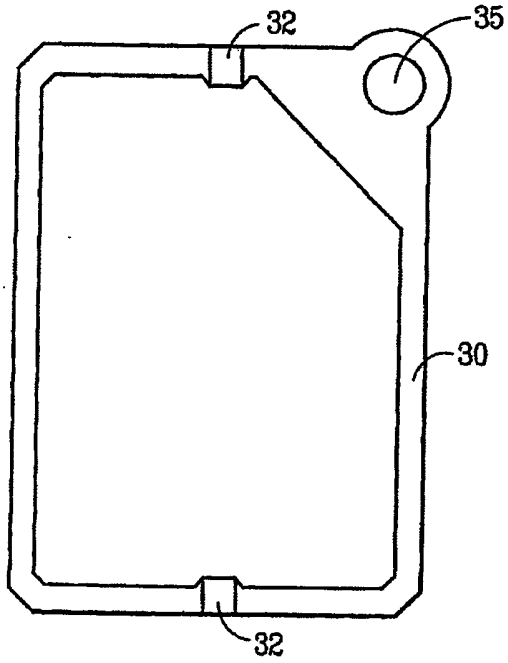


FIG. 7